Europ. J. Combinatorics (1982) **3**, 1–7

On the Number of Points Caps Obtained from an Elliptic Quadric of $PG(3, q)$

L. MARIA ABATANGELO*

Caps K of $PG(3, q)$ with properties (1) and (2) have been studied in [1, 2, 3]. The Segre estimate for the number $|K|$ is that $|K| \leqslant |K \cap Q| + q + 1$. In this paper, it is proved that if $q+1 = 2p$, $p(\geqslant 5)$ an odd prime, then $|K| \leqslant |K \cap Q| + 4$. A general construction for complete $(q+5)/2$-arcs with $q \equiv 1 (\text{mod } 4)$ is also discussed.

1. INTRODUCTION

In $PG(3, q)$ a *cap* is a set of k points no three of which are collinear. A cap K is *complete* if it is not contained in any cap K'.

Several papers have been devoted to the study of caps K of $PG(3, q)$ with the following properties:

$$K \not\subset Q, \tag{1}$$

$$|K \cap Q| = (q^2 + q + 2)/2, \tag{2}$$

where Q is an elliptic quadric of $PG(3, q)$.

A fundamental result of Segre (cf. [8, p. 73]), which has been the starting point for various other questions in this direction, is the following:

$$|K| \leqslant |K \cap Q| + q + 1.$$

On the other hand, complete caps K satisfying (1) and (2) with

$$\begin{aligned} |K| = |K \cap Q| + 1 \quad & \text{for } q \text{ even (cf. [1, 2]),} \\ & \text{for } q \equiv 3 \ (\text{mod } 4) \text{ (cf. [8, p. 73]),} \\ |K| \geqslant |K \cap Q| + 2 \quad & \text{for } q \neq 3 \text{ and } q \not\equiv 1 \ (\text{mod } 3) \text{ (cf. [8, p. 73])} \end{aligned}$$

have been constructed.

In this paper, the following theorem is proved.

THEOREM. *If $q+1 = 2p$, p an odd prime and $q \geqslant 9$, then*

$$|K| \leqslant |K \cap Q| + 4.$$

Finally a construction for complete $(q+5)/2$-arcs, with $q \equiv 1$ (mod 4) is also discussed in this paper (Section 5).

2. REGULAR AND PSEUDOREGULAR CHORDS WITH RESPECT TO AN ELLIPSE OF AN AFFINE GALOIS PLANE $A(2, q)$, q ODD

In $AG(2, q)$, we define the ratio (P_1P_2P) of any three distinct collinear points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P = (x, y)$, with $x = x_2 + k(x_1 - x_2)$ and $y = y_2 + k(y_1 - y_2)$ as follows:

$$(P_1P_2P) = (1-k)/k.$$

* Research partially supported by G.N.S.A.G.A. (C.N.R.). The author wishes to thank G. Korchmáros, visiting professor at the University of Bari, for helpful discussions.

0195–6698/82/010001+07 $02.00/0

Let P_1, P_2 be any two *distinct* points of $AG(2, q)$. Following Segre [11; 12, Part III] the *affine segment* P_1P_2 is the set of all the points P of the line P_1P_2, for which

$$(P_1P_2P) \in \Delta.$$

Furthermore, a point P of P_1P_2 is called *external* or *internal* to the affine segment P_1P_2 according to whether the ratio (P_1P_2P) is a square or a non-square in $GF(q)$.

Let C be an ellipse of $AG(2, q)$. A chord P_1P_2 of C is called *regular* (resp. *pseudoregular*), if each point P, not on C, satisfies the condition (a) (resp. (b)):

(a) P is external or internal to the affine segment P_1P_2 according to whether it is external or internal to C;

(b) P is external or internal to the affine segment P_1P_2 according to whether it is internal or external to C.

By a remarkable theorem of Segre [11, Section 10], we have the following proposition.

PROPOSITION 2.1. *Each chord of C is either regular or pseudoregular.*

We will give a criterion (cf. Proposition 2.5) under which a chord of C is regular or pseudoregular. In order to do this, we need some preparation.

Let $GF(q^2)$ be a quadratic extension of $GF(q)$. Let $x^2 - s$ be an irreducible polynomial over $GF(q)$. Then

$$GF(q^2) = \{x + iy \mid (x, y) \in GF(q)^2 \text{ and } i^2 = s\}.$$

For every $z = x + iy \in GF(q^2)$ we define $\bar{z}$ as $\bar{z} = x - iy$. The elements $z = x + iy$ of $GF(q^2)$ for which

$$z\bar{z} = (x + iy)(x - iy) = 1$$

form a cyclic group G of order $q + 1$. Let g be a generator of G. We put

$$G_{\square} = \{g^2, g^4, \ldots, g^{q+1} = 1\} \text{ and } G_{\triangle} = \{g, g^3, \ldots, g^q\}.$$

For every $w \in G$, we define a mapping f_w of $GF(q^2)$ into itself by

$$f_w\colon z \to zw.$$

Let $\Phi = \{f_w \mid w \in G\}$. It is easy to show the following:

PROPOSITION 2.2

(a) $f_w(G) = G$.

(b) $\left.\begin{matrix} f_w(G_{\square}) = G_{\square} \\ f_w(G_{\triangle}) = G_{\triangle} \end{matrix}\right\} \Leftrightarrow w \in G_{\square}.$

(c) $\left.\begin{matrix} f_w(G_{\triangle}) = G_{\square} \\ f_w(G_{\square}) = G_{\triangle} \end{matrix}\right\} \Leftrightarrow w \in G_{\triangle}.$

(d) *Φ is a group which is isomorphic to G.*

(e) *$\Phi_{\square} = \{f_w \mid w \in G_{\triangle}\}$ is a subgroup of order $(q + 1)/2$.*

(f) *Φ acts sharply transitively on G.*

(g) *$\Phi_{\square}$ has exactly two orbits on G*: $G_{\square}$ and $G_{\triangle}$.

Let us consider the ellipse C with equation: $x^2 - sy^2 = 1$. The mapping $(x, y) \to x + iy$ defines a bijection between the points of C and the elements of G.

Putting

$$C_{\square} = \{(x, y) \mid x + iy \in G_{\square}\} \quad \text{and} \quad C_{\triangle} = \{(x, y) \mid x + iy \in G_{\triangle}\}$$

we prove the following:

PROPOSITION 2.3. *If* (x, y) *is an arbitrary point of* C, *then*
(a) *there exists a pair* (a, b) *such that* a *and* b *belong to* $GF(q^2)$, $a^2+sb^2=x$, $2ab=y$, $a^2-sb^2=1$.
(b) $(x, y)\in C_\square \Leftrightarrow a, b\in GF(q)$
(c) $(x, y)\in C_\triangle \Leftrightarrow a, b\in GF(q^2)\backslash GF(q)$.

PROOF. For any $(x, y)\in C$, let us consider the system

$$\begin{cases} a^2+sb^2=x \\ 2ab=y \\ a^2-sb^2=1 \end{cases} \tag{3}$$

over the algebraic closure of $GF(q)$. It is easy to see that if (a, b) is a solution of (3), then

$$a^2=(x+1)/2 \quad \text{and} \quad b^2=y^2/2(x+1) \quad \text{for } x\neq -1,$$
$$a=0 \quad \text{and} \quad b=-1/s \quad \text{for } x=-1.$$

As $x+1$, y^2, s belong to $GF(q)$, (a) follows. Next we prove (b). If $(x, y)\in C_\square$, then there is $t\in GF(q^2)$ such that $t^2=x+iy$. Note that $t^2=x+iy$ implies $\bar{t}^2=x-iy$. It is easy to see that then $a=(t+\bar{t})/2$, $b=(t-\bar{t})/2i$ is a solution of (3). As $t\in GF(q^2)$, we have that a and b belong to $GF(q)$.

Conversely, suppose that (3) admits a solution (a, b), with $a, b\in GF(q)$. By the first two equations of (3), we have then $(a+ib)^2=x+iy$. By the last equation of (3), $a+ib\in G$. Thus $(x, y)\in C_\square$.

It is clear that (c) is a consequence of (a) and (b). For every a, b elements of $GF(q)$, such that $a^2-sb^2=1$, let us consider the collineation $R_{a,b}$ of $AG(2, q)$ defined by

$$\begin{cases} x'=ax+sby \\ y'=bx+ay. \end{cases}$$

It is easy to show the following:

PROPOSITION 2.4. *Let* $z\in G$ *and* $(x, y)\in C$, *where* $z=x+iy$. *If* $f_w(z)=z'$ *and* $R_{a,b}(x, y)=(x', y')$, *then* $w=a+ib\Leftrightarrow z'=x'+iy'$.

Since there is a bijection between C and G and an isomorphism between Φ and $\mathcal{R}$, by comparison with Proposition 2.2 we have the following:

PROPOSITION 2.5. *The collineations* $R_{a,b}$ *satisfy the following properties*:
(a) $R_{a,b}(C)=C$.
(b) $\left.\begin{matrix} R_{a,b}(C_\square)=C_\square \\ R_{a,b}(C_\triangle)=C_\triangle \end{matrix}\right\}\Leftrightarrow a+ib\in G_\square$.
(c) $\left.\begin{matrix} R_{a,b}(C_\square)=C_\triangle \\ R_{a,b}(C_\triangle)=C_\square \end{matrix}\right\}\Leftrightarrow a+ib\in G_\triangle$.
(d) $\mathcal{R}=\{R_{a,b}\mid a+ib\in G\}$ *is a group isomorphic to* Φ.
(e) $\mathcal{R}_\square=\{R_{a,b}\mid a+ib\in G_\square\}$ *is a subgroup of* $\mathcal{R}$ *of order* $(q+1)/2$.
(f) $\mathcal{R}$ *acts on* C *as* Φ *on* G.
(g) $\mathcal{R}_\square$ *has exactly two orbits*: $C_\square$ *and* $C_\triangle$.

PROPOSITION 2.6. *Let P_1P_2 be any chord of C.*
(a) *P_1P_2 is regular $\Leftrightarrow P_1, P_2 \in C_\square$ or $P_1, P_2 \in C_\triangle$.*
(b) *P_1P_2 is pseudoregular $\Leftrightarrow P_1 \in C_\square$, $P_2 \in C_\triangle$ or $P_1 \in C_\triangle$, $P_2 \in C_\square$.*

PROOF. By Proposition 2.5 (a) every $R_{a,b}$ maps into itself the set of all external points of C as well as the set of all internal points of C. Moreover, $R_{a,b}$ respects the ratio (P_1P_2P). Therefore every $R_{a,b}$ leaves invariant the set of all regular chords as well as the set of all pseudoregular chords. On the other hand, by Proposition 2.5 (b), (c), every $R_{a,b}$ leaves invariant $C_\square$ and $C_\triangle$ or interchanges $C_\square$ and $C_\triangle$. It follows that if a chord P_1P_2 verifies (a) (resp. (b)), then also every chord $P_1'P_2'$, with $P_1' = R_{a,b}(P_1)$ and $P_2' = R_{a,b}(P_2)$, verifies (a) (resp. (b)). By Proposition 2.5(f), $\mathscr{R}$ acts transitively on the points of C. Thus, without loss of generality, we can assume that $P_1 = (1, 0)$.

Let $P(\xi, \eta)$ be any point of P_1P_2, not on C. By Segre (cf. [11, Section 5, p. 296]), then

$$P(\xi, \eta) \text{ is external to } C \Leftrightarrow \sigma(P) \in \square,$$

$$P(\xi, \eta) \text{ is external to } C \Leftrightarrow \sigma(P) \in \triangle,$$

where $\square$ is the set of squares, $\triangle$ is the set of non-squares and

$$\sigma(P) = -s(\xi^2 - s\eta^2 - 1).$$

Let $k(P) = (P_1P_2P)$. Then the chord P_1P_2 of C is regular or pseudoregular according to whether $k(P)$ and $\sigma(P)$ satisfy the conditions (a') or (b'), where
(a') $k(P) \in \square \Leftrightarrow \sigma(P) \in \square$ and $k(P) \in \triangle \Leftrightarrow \sigma(P) \in \triangle$,
(b') $k(P) \in \square \Leftrightarrow \sigma(P) \in \triangle$ and $k(P) \in \triangle \Leftrightarrow \sigma(P) \in \square$
for every point P of P_1P_2 not on C.

Therefore, as $P_1 = (1, 0)$ and thus $P_1 \in C_\square$, we have to prove

$$P_2 \in C_\square \Leftrightarrow \text{(a') holds,} \tag{3}$$

$$P_2 \in C_\triangle \Leftrightarrow \text{(b') holds.} \tag{3'}$$

Let $P_2 = (x_2, y_2)$. Then

$$\xi = (1 - kx_2)/(1 - k), \qquad \eta = -ky_2/(1 - k).$$

Thus $\sigma(P) = 2ks(x_2 - 1)/(1 - k)^2$. On the other hand, from Proposition 2.1 it follows that $a^2, b^2 \in GF(q)$, such that $x_2 = a^2 + sb^2$, where a and b are elements of $GF(q)$ or $GF(q^2)\backslash GF(q)$ according to whether

$$P_2 \in C_\square \quad \text{or} \quad P_2 \in C_\triangle.$$

Hence $\sigma(P) = 4s^2b^2k/(1 - k)^2$, where $b^2 \in \square$ or $b^2 \in \triangle$ according to whether $P_2 \in C_\square$ or $P_2 \in C_\triangle$. As $4s^2/(1 - k)^2$ is a square, (3) and (3') follow.

3. REGULAR AND PSEUDOREGULAR POINTS WITH RESPECT TO AN ELLIPSE OF AN AFFINE GALOIS PLANE $AG(2, q)$, q ODD

Let C be an ellipse of $AG(2, q)$. Following Segre (cf. [11, Section 13]) a point P of $AG(2, q)$, not on C, is called *regular* (resp. *pseudoregular*) with respect to C, if it satisfies conditions (i) and (ii) (resp. (iii)):
(i) if P is external to C, then the chords of C through P are all regular;
(ii) if P is internal to C, then the chords of C through P are all regular or all pseudoregular;
(iii) if P is external to C, then each chord of C through P is pseudoregular.

PROPOSITION 3.1 (Segre [11, Section 17]). *The unique regular point with respect to C is the centre of C.*

PROPOSITION 3.2 (Segre [11], Kàrteszi [5], Debroey [3]). *If $q \geqslant 9$, there are no pseudoregular points with respect to C.*

4. k-ARCS OF $AG(2, q)$ WHICH MEET C IN $C_\square$ OR IN $C_\triangle$

PROPOSITION 4.1. *Let $\gamma = C_\square$ or $\gamma = C_\triangle$. For any point of $AG(2, q)$, $q \geqslant 9$, $\gamma \cup \{P\}$ is an arc if and only if P lies on $C \setminus \gamma$ or $q \equiv 1 \pmod 4$ and P is the centre of C.*

PROOF. Let P be any point of $AG(2, q)$ not on C. It is clear that $\gamma \cup \{P\}$ is an arc if and only if each chord of C through P is pseudoregular with respect to C.

First suppose that P is an external point to C. Then P is a pseudoregular point with respect to C (cf. Section 3(iii)). By Proposition 3.2, there are no pseudoregular points with respect to C. Therefore we may suppose that P is an internal point to C. Then P is a regular point with respect to C (cf. Section 3(ii)). By Proposition 3.1, the unique regular point with respect to C is the centre of C. We have to prove that $\gamma \cup \{0\}$ is an arc if and only if $q \equiv 1 \pmod 4$. The chord P_1P_2, where $P_1 = (1, 0)$ and $P_2 = (-1, 0)$, passes through 0, and P_1P_2 is regular or pseudoregular with respect to C according to whether $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$. In fact, as P_1 belongs to C and $g^{(q+1)/2} = 1 - i$, P_2 belongs to $C_\square$ or $C_\triangle$ according to $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$. By Section 3(ii), it follows that the chords of C through 0 are all regular or all pseudoregular according to whether $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$. Thus $\gamma \cup \{0\}$ is an arc if and only if $q \equiv 1 \pmod 4$.

5. COMPLETENESS CRITERIA FOR k-ARCS WITH $(q+1)/2$ POINTS ON A CONIC

Let $PG(2, q)$ be the projective closure of $AG(2, q)$. For every point $D(u, v, 0)$ at infinity, we define an involutory homology $L_{u,v}$ as follows

$$\begin{cases} x' = Ux - sVy \\ y' = Vx - Uy, \end{cases}$$

where $U = (u^2 + sv^2)/(sv^2 - u^2)$ and $V = 2uv/(sv^2 - u^2)$.

We omit the proof of the following proposition because it is easy.

PROPOSITION 5.1

(a) *$D(u, v, 0)$ is the centre of $L_{u,v}$.*

(b) *The polar d of $D(u, v, 0)$ with respect to C is the axis of $L_{u,v}$.*

(c) *$L_{u,v}(C) = C$.*

(d) *$D(u, v, 0)$ is internal to C if and only if $sv^2 - u^2$ is a square.*

(e) *Let $L_{m,n}$ be an involutory homology with equations:*

$$\begin{cases} x' = Mx - sNy \\ y' = Nx - My. \end{cases}$$

Then $L_{u,v}L_{m,n} = R_{a,b}$, where $a = UM - sVN$ and $b = VM - UN$.

(f) *If both $D(u, v, 0)$ and $D'(m, n, 0)$ are internal points to C, then*

$$L_{u,v}L_{m,n} = R_{a,b},$$

where

$$a=[(svn-um)^2+s(vm-un)^2]/(sv^2-u^2)(sn^2-m^2)$$
$$b=2(svn-um)(vm-un)/(sv^2-u^2)(sn^2-m^2)$$
$$a+ib\in G_{\square}.$$

PROPOSITION 5.2. *Let θ be a $(q+1)/2$-arc contained in C. For any point $D(u, v, 0)$ at infinity, $\theta\cup\{D\}$ is an arc if and only if $L_{u,v}$ interchanges θ and $C\backslash\theta$.*

PROOF. Let P_1, P_2 be two points on C. P_1, P_2 and D are three collinear points if and only if $L_{u,v}(P_1)=P_2$.

Then we have the following:

COROLLARY 5.1. *Let θ be a $(q+1)/2$-arc contained in C. For any two distinct points $D(u, v, 0)$ and $D'(m, n, 0)$, $\theta\cup\{D, D'\}$ is an arc if and only if $L_{u,v}L_{m,n}$ maps θ into itself.*

PROPOSITION 5.3. *Let θ be a $(q+1)/2$-arc contained in C. If $D(u, v, 0)$ and $D'(m, n, 0)$ are two distinct internal points to C, such that $\theta\cup\{D, D'\}$ is an arc, then, provided $q+1=2p$, p an odd prime,*

$$\theta=C_{\square} \quad or \quad \theta=C_{\triangle}.$$

PROOF. By Proposition 5.1(f), we can put $L_{u,v}L_{m,n}=R_{a,b}$. As both D and D' are internal points to C, we have actually $a+ib\in G_{\square}$, i.e. $R_{a,b}\in\mathcal{R}_{\square}$. Since by assumption $q+1=2p$ and p is prime, by Proposition 2.5(e) we have that $R_{a,b}$ is a generator of $\mathcal{R}_{\square}$. Thus

$$\mathcal{R}_{\square}=\{R^j_{a,b}\mid j=1,2,\ldots,p\}. \tag{4}$$

As $a+ib\in G_{\square}$, by Corollary 5.1, we have $R_{a,b}(\theta)=\theta$. Thus $R^j_{a,b}(\theta)=\theta$ for every $j=1,2,\ldots,p$. Therefore, by (4),

$$\mathcal{R}_{\square}(\theta)=\theta.$$

By Proposition 2.5(g), $\theta=C_{\square}$ or $\theta=C_{\triangle}$.

PROPOSITION 5.4. *Let C be an irreducible conic of $PG(2, q)$, with $q+1=2p$ and p an odd prime. Let θ be a $(q+1)/2$-arc contained in C. If D and D' are two distinct internal points with respect to C, such that $\theta\cup\{D, D'\}$ is an arc, then $\theta\cup\{D, D'\}$ is complete.*

PROOF. It is clear that DD' is an external line to C. Let $AG(2, q)$ be the affine plane obtained from $PG(2, q)$ by deleting the line DD'. As $DD'\cap C=\emptyset$, C is an ellipse of $AG(2, q)$. Then we may assume the coordinate system of $AG(2, q)$ so that the equation of C is $x^2-sy^2=1$ and apply Proposition 5.3. Then $\theta=C_{\square}$ or $\theta=C_{\triangle}$. We have to prove that neither $C_{\square}\cup\{D, D', P\}$ nor $C_{\triangle}\cup\{D, D', P\}$ is an arc, for any affine point not on C. By Proposition 4.1, we can assume that P is the centre of C or $P\in C-C_{\square}$ (resp. $P\in C-C_{\triangle}$). The latter case cannot occur in our situation by Propositions 5.2 and 5.1 (a), (c). Then suppose that P is the centre of C. By Proposition 5.1(d), PD is a chord of C. By Propositions 5.2 and 5.1(a), (c), PD meets $C_{\square}$ as well as $C_{\triangle}$. This proves our proposition.

6. The Proof of the Theorem

Let us consider any plane π of $PG(3, q)$. Firstly, suppose that π is a tangent plane to Q. Then, by a result of Segre (cf. [8, p. 73]), $\pi \cap K$ has at most three points not on Q. We can assume that π is a secant plane to Q. Suppose that π contains some points of K not on Q. If $\pi \cap K$ contains at least one external point to $\pi \cap Q$, then $|Q \cap K \cap \pi| = (q+3)/2$. By a theorem of Korchmàros [6] (see Pellegrino [7]) there exist at most two points not on Q. Therefore, we can suppose that every point of $\pi \cap K$ not on Q is internal to $\pi \cap Q$. This case is considered in the present paper. By Proposition 5.3, if $q+1=2p$, with p odd prime and $q \geqslant 9$, there exist in $\pi \cap K$ at most two points not on Q.

Suppose that $|K| \geqslant |K \cap Q| + 2$. Let $D, D' \in \{K - Q\}$. As there are exactly two tangent planes to Q through DD' and every other plane through DD' is secant to Q, from the above theorems it follows that $|K| \leqslant |K \cap Q| + 4$ provided $q+1=2p$, p an odd prime and $q \geqslant 9$.

References

1. L. M. Abatangelo, Calotte complete in uno spazio di Galois $PG(3, q)$, q pari, *Atti Sem. Mat. Fis. Univ. Modena* (to appear).
2. C. Di Comite, Calotte complete in un $S_{3,q}$, con q pari, *Atti Accad. Naz. Lincei Rend.* **46** (1969), 385–389.
3. I. Debroey, A remark on a result of B. Segre concerning pseudoregular points of an elliptic quadric of $AG(2, q)$, q odd, *J. Geom.* **14** (1980), 159–163.
4. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.
5. F. Kàrteszi, Su una congettura di Seppo Ilkka, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **20** (1977), 167–175.
6. G. Korchmàros, Osservazioni sui risultati de B. Segre relativi ai k-archi contenenti $k-1$ punti di una ovale, *Atti Accad. Naz. Lincei Rend.* **56** (1974), 541–549.
7. G. Pellegrino, Un'osservazione sul problema dei k-archi completi in $S_{2,q}$, con $q \equiv 1 \pmod 4$, *Atti Accad. Naz. Lincei Rend.* **63** (1977), 33–44.
8. B. Segre, Le geometrie di Galois, *Ann. Mat. Pura Appl.* **48** (1959), 1–97.
9. B. Segre, *Lectures on Modern Geometry*, Cremonese, Roma, 1960.
10. B. Segre, Introduction to Galois geometries (J. W. P. Hirschfeld, ed.), *Atti Accad. Naz. Lincei Mem.* **8** (1967), 133–236.
11. B. Segre, Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois, *Ann. Mat. Pura Appl.* **96** (1973), 289–337.
12. B. Segre, Incidence structures and Galois geometries, with special regard to regular involutive correspondences, arcs, caps, segments and conics. *Teorie Combinatorie Volume I*, Accademia Nazionale dei Lincei, Rome, 1973, pp. 331–369.

Received 14 September 1981 and in revised form 20 November 1981

L. M. Abatangelo
Istituto di Geometria, Università degli Studi,
Via Nicolai, 2, 70121 Bari, Italy